RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: CIT-R06

Securing the Food Supply: A Cyber Threat Briefing on the Food and Ag Sector

Jonathan Braley

Director
Food and Agriculture-ISAC

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

About Me

- Jonathan Braley
- Director - Food and Agriculture-ISAC

Food and Ag-ISAC

- Information Sharing and Analysis Centers (ISACs) support their respective critical sectors to assist members in sharing timely and actionable cyber threat intelligence.
- Information Technology-ISAC (IT-ISAC)
  - Formed a Food and Agriculture Special Interest Group (SIG) in 2013.
- May 2023 - Formal Food and Ag-ISAC was formed.
  - Members of the Food and Ag-ISAC are also members of the IT-ISAC.

RSAC 2025 Conference

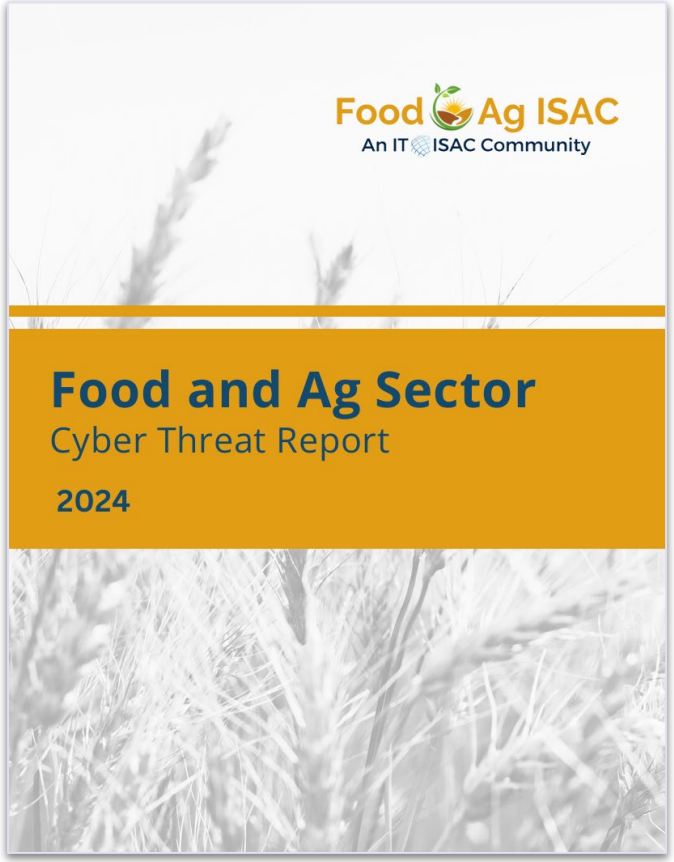
Cyber Threat Briefing on the Food and Ag Sector

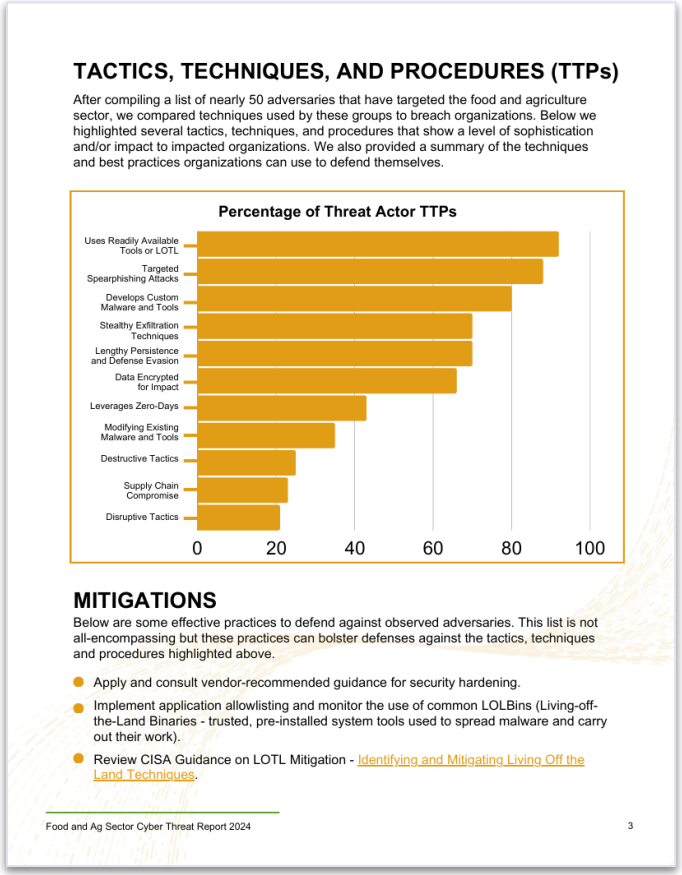
Predictive Adversary Scoring System (PASS)

- PASS was developed by the IT-ISAC and Food and Ag-ISAC.
- The tool uses several metrics to “score” a set of adversaries known to target a specific sector, vertical, or individual organization.
  - **Level of Activity**
    - How recently has the group been active
  - **Frequency of Sector Targeting**
    - How often has the adversary attacked the sector in the past
  - **Sophistication/Impact**
    - Set of tactics, techniques, and procedures that show a level of sophistication or impact
  - **Motivation**
    - Financial, Geopolitical, Ideological, Recognitional

Predictive Adversary Scoring System (PASS)

- Public report “Food and Ag Sector 2024 Cyber Threat Report”





TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

After compiling a list of nearly 50 adversaries that have targeted the food and agriculture sector, we compared techniques used by these groups to breach organizations. Below we highlighted several tactics, techniques, and procedures that show a level of sophistication and/or impact to impacted organizations. We also provided a summary of the techniques and best practices organizations can use to defend themselves.

MITIGATIONS

Below are some effective practices to defend against observed adversaries. This list is not all-encompassing but these practices can bolster defenses against the tactics, techniques and procedures highlighted above.

- Apply and consult vendor-recommended guidance for security hardening.
- Implement application allowlisting and monitor the use of common LOLBins (Living-off-the-Land Binaries - trusted, pre-installed system tools used to spread malware and carry out their work).
- Review CISA Guidance on LOTL Mitigation - Identifying and Mitigating Living Off the Land Techniques.

Food and Ag Sector Cyber Threat Report 2024 3

Predictive Adversary Scoring System (PASS)

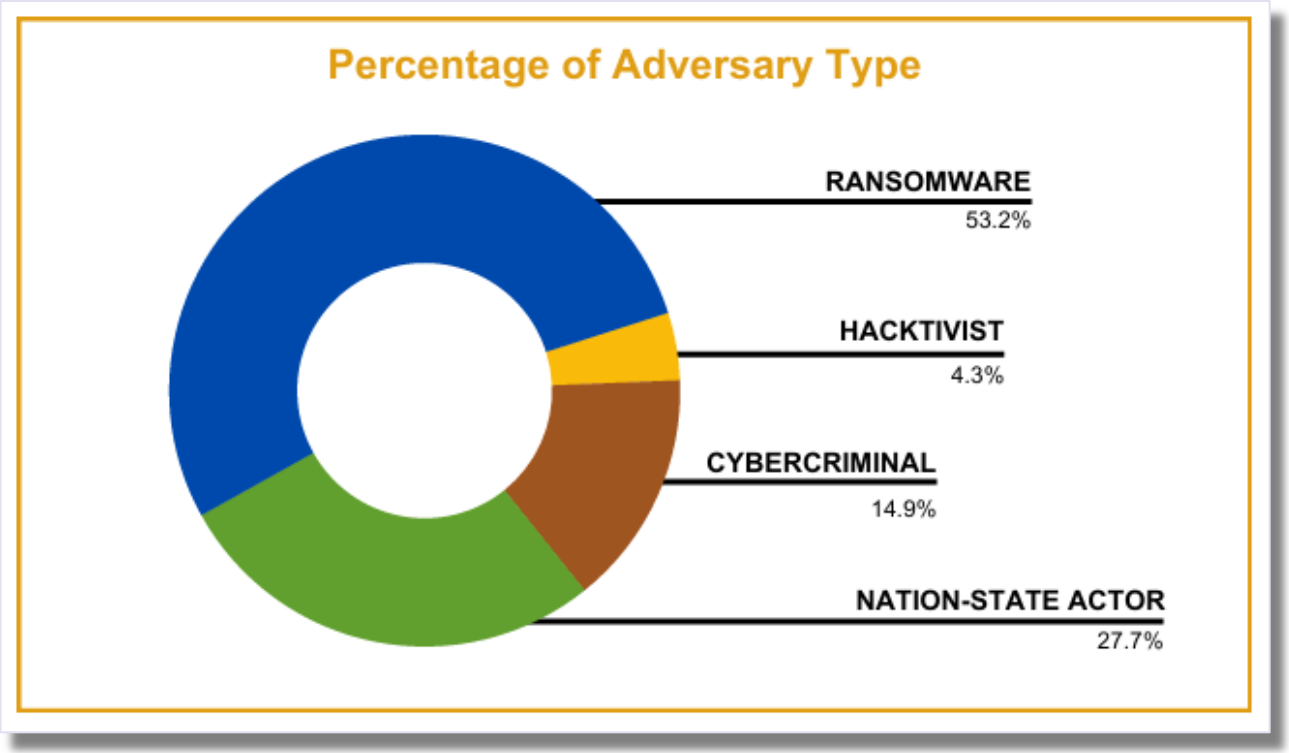
- Who were the victims?
  - Various organizations across the Food and Agriculture sector
    - Agribusinesses
    - Food processors
    - Food distributors
    - Food and beverage companies
    - Small and medium sized farms
    - Restaurants
    - Grocery chains
    - Farming cooperatives
    - And more…

RSAC 2025 Conference

Threat Report Findings

Threat Report Findings

- Roughly 50 adversaries were found to target the Food and Agriculture sector
  - Ransomware Groups
  - Nation-State Actors
  - Cybercriminals
  - Hacktivists

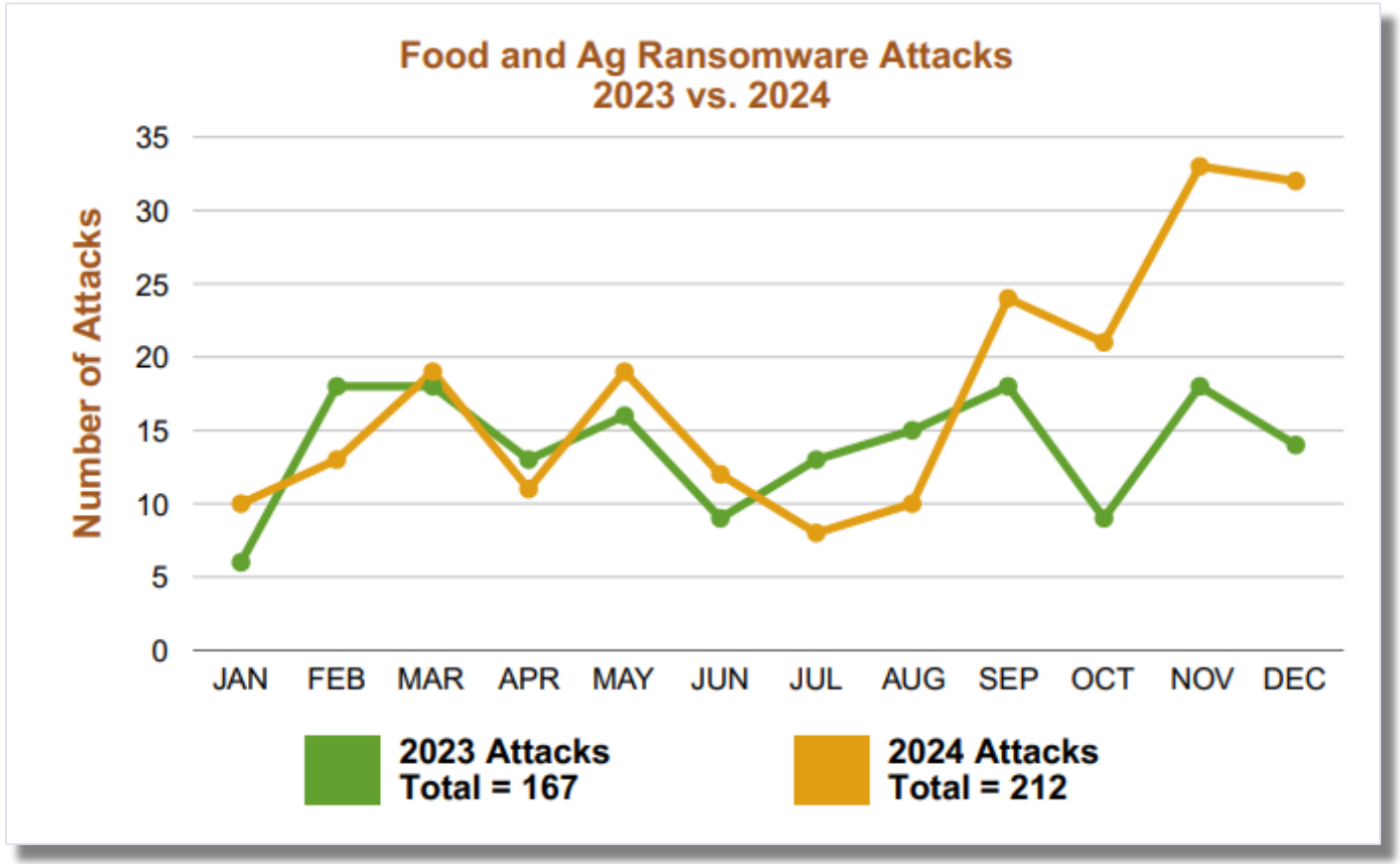


RSAC 2025 Conference

Ransomware

Threat Report Findings

- Ransomware
  - 53% of threat actors, **not specific attacks**, were ransomware actors.



Top Impacted Sectors

2023
3,008 Observed Attacks

Critical Manufacturing	468
Commercial Facilities	399
Financial Services	375
Health Care	298
Information Technology	284
Food and Agriculture	**167**

2024
3,500 Observed Attacks

Critical Manufacturing	733
Commercial Facilities	614
Health Care	332
Information Technology	299
Financial Services	269
Food and Agriculture	**212**

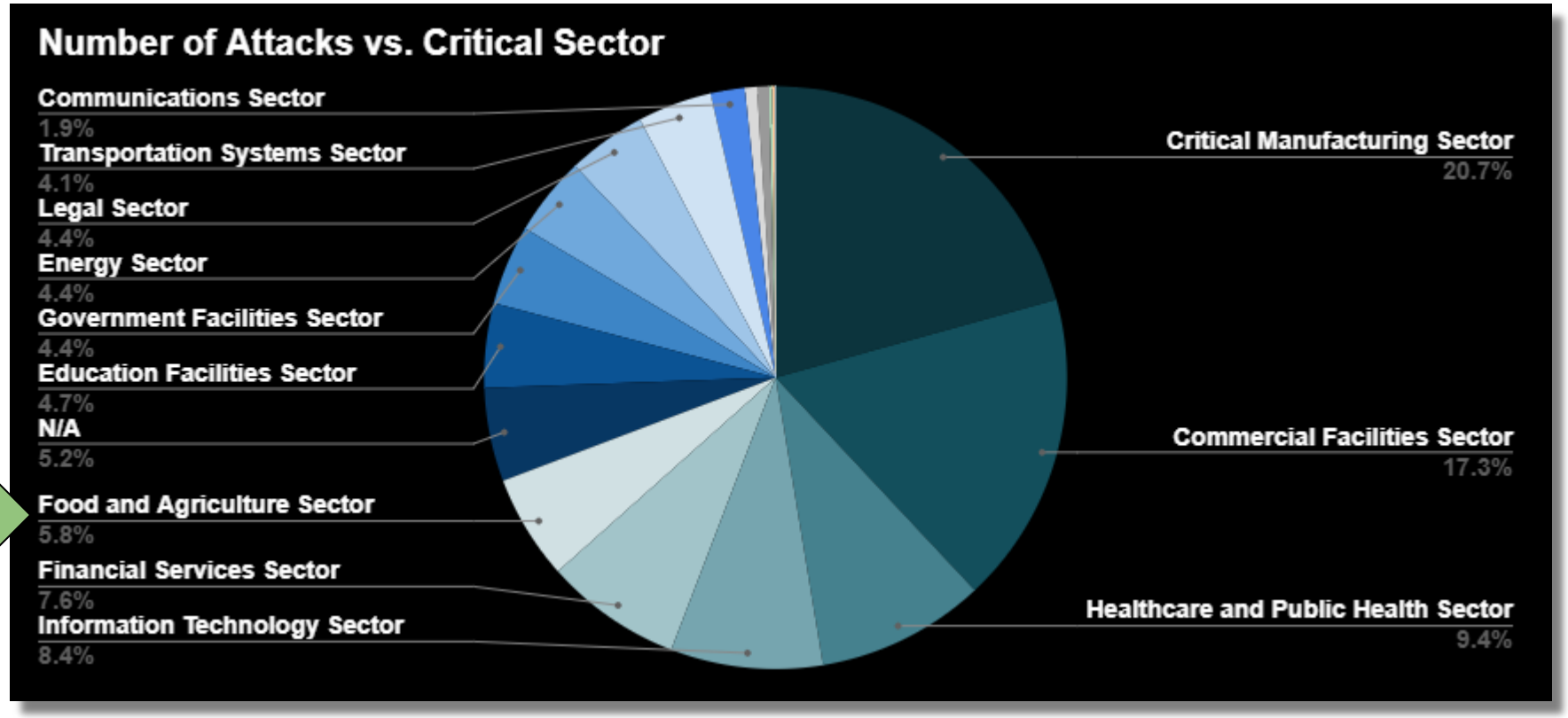
Ransomware Impacts

- Just-in-time delivery of products and services.
- Operational technology and manufacturing environments.
- Robust supply chain
- Cross sector-interdependencies
  - Water
  - Oil and Natural Gas
  - Transportation
  - Maritime
  - Etc.

Ransomware Tracker

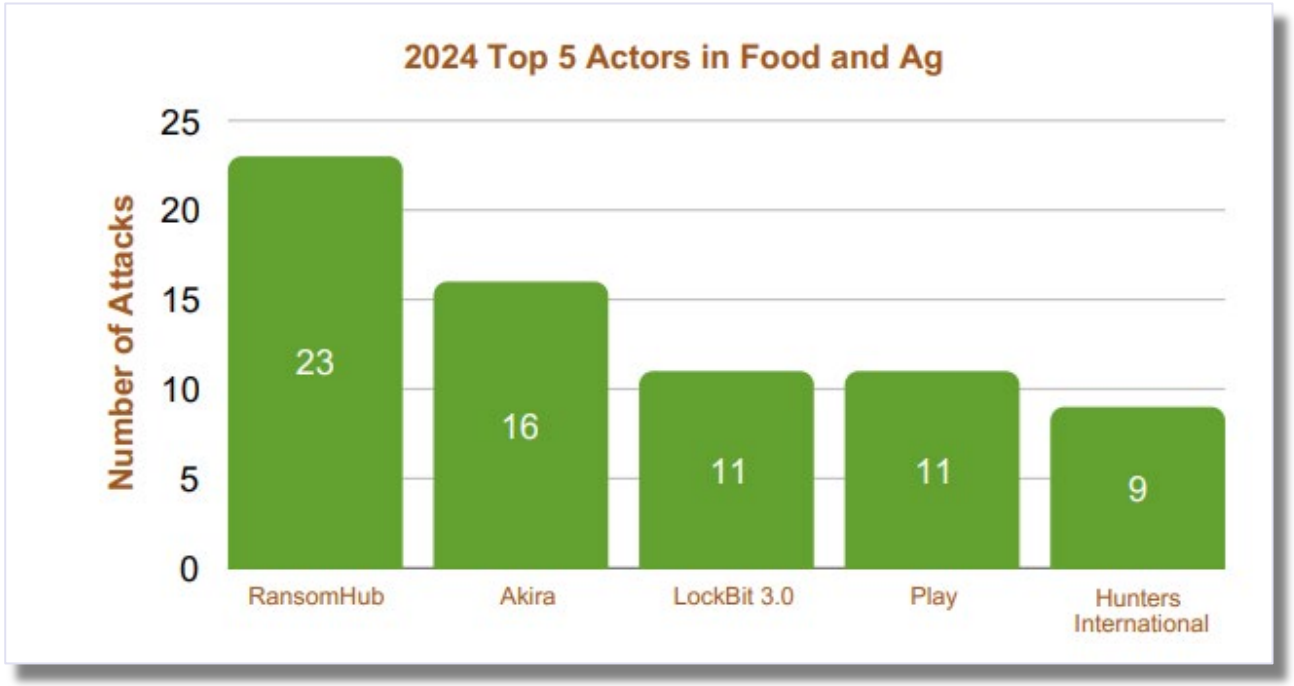
- In 2024, the IT-ISAC and Food and Ag-ISAC tracked nearly 3,500 attacks across all critical sectors globally.

5.8%



Ransomware Findings

- Opportunistic Attacks
  - Phishing Attacks
  - Initial Access Brokers
  - Scanning for Exposed Vulnerabilities



Notable Ransomware Attacks

- **JBS Foods (2021)** - JBS, one of the world's largest meat processors, had to shut down operations in the U.S., Canada, and Australia.
- **New Cooperative (2021)** - A U.S.-based grain cooperative suffered an attack, affecting its ability to manage grain logistics and supply.
- **Schreiber Foods (2021)** - A Wisconsin-based dairy company had to halt production due to a cyberattack.
- **Crystal Valley Cooperative (2021)** - The Minnesota-based cooperative suffered an attack that disrupted grain and feed operations.
- **Dole (2023)** - Dole temporarily shut down North American operations after the attack.
- **Blue Yonder Attack (November 2024)** - Impacted Major retailers including Starbucks, Morrisons, and Sainsbury's.
- **Krispy Kreme (November 2024)** - A cyberattack disrupted Krispy Kreme's online operations and ordering systems in parts of the U.S., leading to significant operational challenges.

Challenges

- Defending against zero-day exploits
- Protecting legacy equipment (operational technology and industrial control systems)
  - Patch management, right to repair, vendor requirement to patch.
  - Halting production to patch systems.
- Large supply chain of partners and suppliers
  - Challenging to help small partners and suppliers who may not have technical staff
  - Shared network infrastructure

Ransomware Takeaways

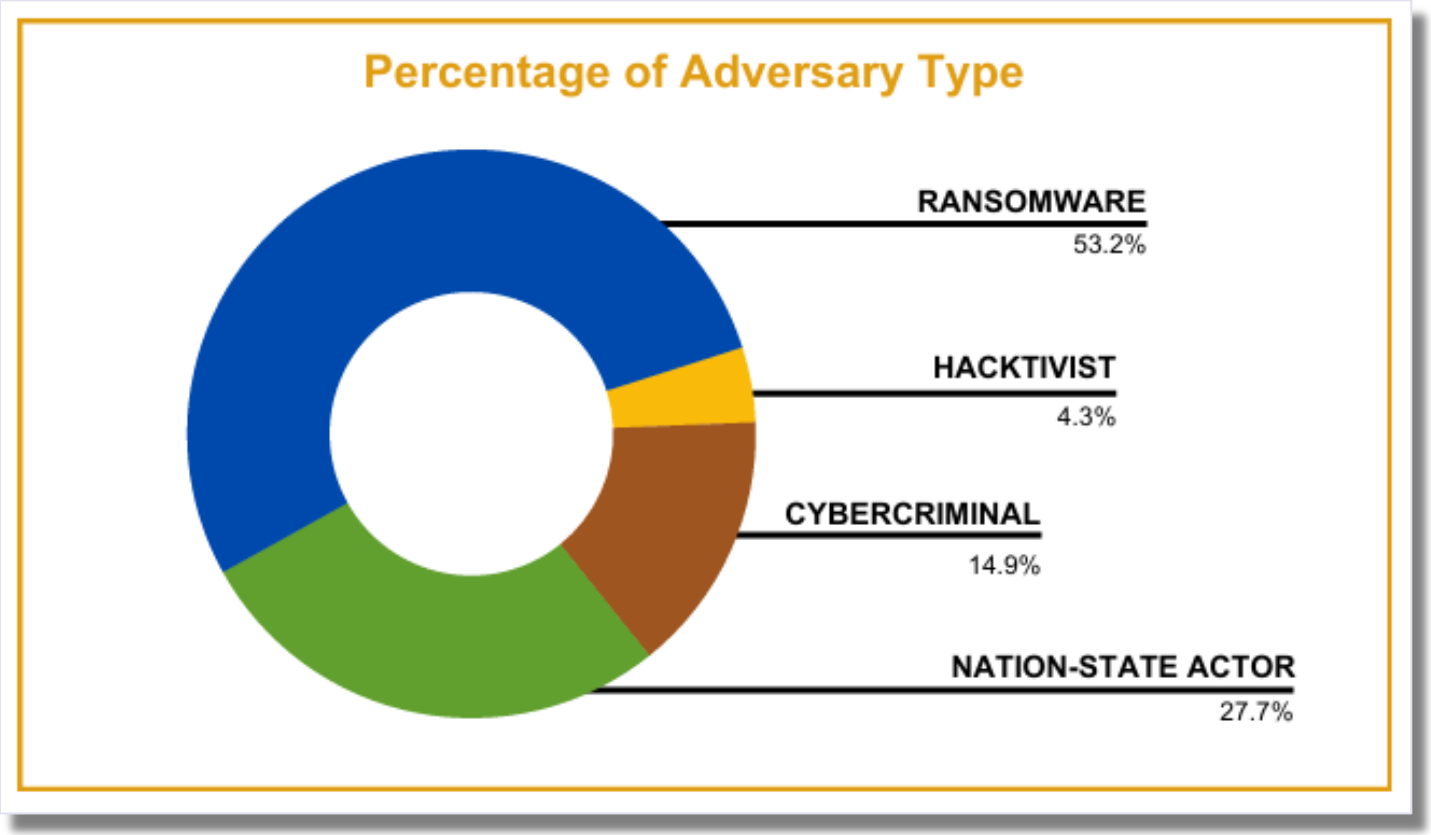
- Attacks against the sector appear opportunistic.
  - Small and large organizations impacted.
- Organizations should continue to improve their risk exposure as it relates to unpatched vulnerabilities and misconfigured systems and services exposed to the Internet.
- User training remains an essential tool in an organization's defenses against ransomware attacks.
  - Phishing emails
  - Breached VPN credentials
  - Stolen credentials

RSAC 2025 Conference

Nation-State Actors

Nation State Actors

- 27% of the threat actors we identified were nation-state sponsored.



Nation-State Motivations

- Motivations to attack the sector:
  - Theft of sensitive intellectual property (IP)
  - Disruptive or destructive attacks
  - Mis/Disinformation to create uncertainty surrounding food and medicine security

Intellectual Property Theft

- Developmental Intellectual property can be incredibly valuable
- Certain nations may be looking to be more self sufficient and may target technologies to assist in their domestic food production.
- Trade leverage and economic advantage

Nation-State Motivations

- Chinese adversaries
  - Interested in long-term developmental intellectual property.
- Russian adversaries
  - Mis/Disinformation campaigns
    - Food and vaccine uncertainty
  - Demotivational attacks
  - Disruptive and destructive attacks against critical infrastructure
- North Korean Adversaries
  - Financially motivated attacks
- Iranian Adversaries
  - Disruptive and destructive attacks against critical infrastructure

Nation-State Motivations

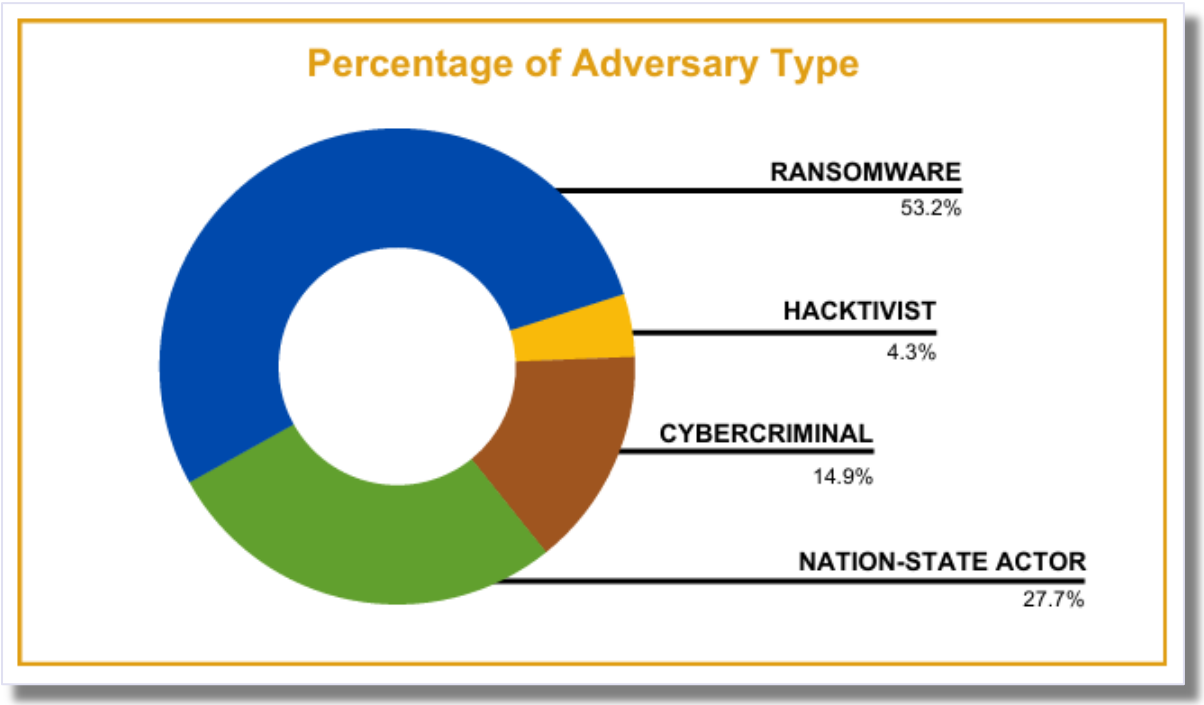
- **China**
  - Targeted U.S. agricultural research institutions, seed companies, and food supply chains.
  - In 2021, the U.S. DOJ charged Chinese nationals with stealing proprietary corn seed technology from U.S. companies.
- **Russia**
  - In 2022–2023, several Ukrainian grain export companies faced cyberattacks that paralyzed logistics and port operations.
  - Sandworm – 2022 Ukraine Grain Silos Attack - Wipers and ransomware-like attacks to sabotage operations rather than demand ransom.
- **North Korea**
  - BlackMatter ransomware, linked to North Korean affiliates, attacked grain cooperatives in the U.S. in 2023.

RSAC | 2025 Conference

Cybercriminal

Cybercriminal

- Distinct from ransomware
  - Other forms of financially motivated theft.
- Can be generic and broad in its targeting.
- Phishing and Spear Phishing
  - Stealer Malware - SmokeLoader, LummaC2, etc.
- Business Email Compromise
  - Invoice fraud
  - Typosquatting domains
- Using search engine advertising (malvertising) to masquerade as corporate login pages



Artificial Intelligence

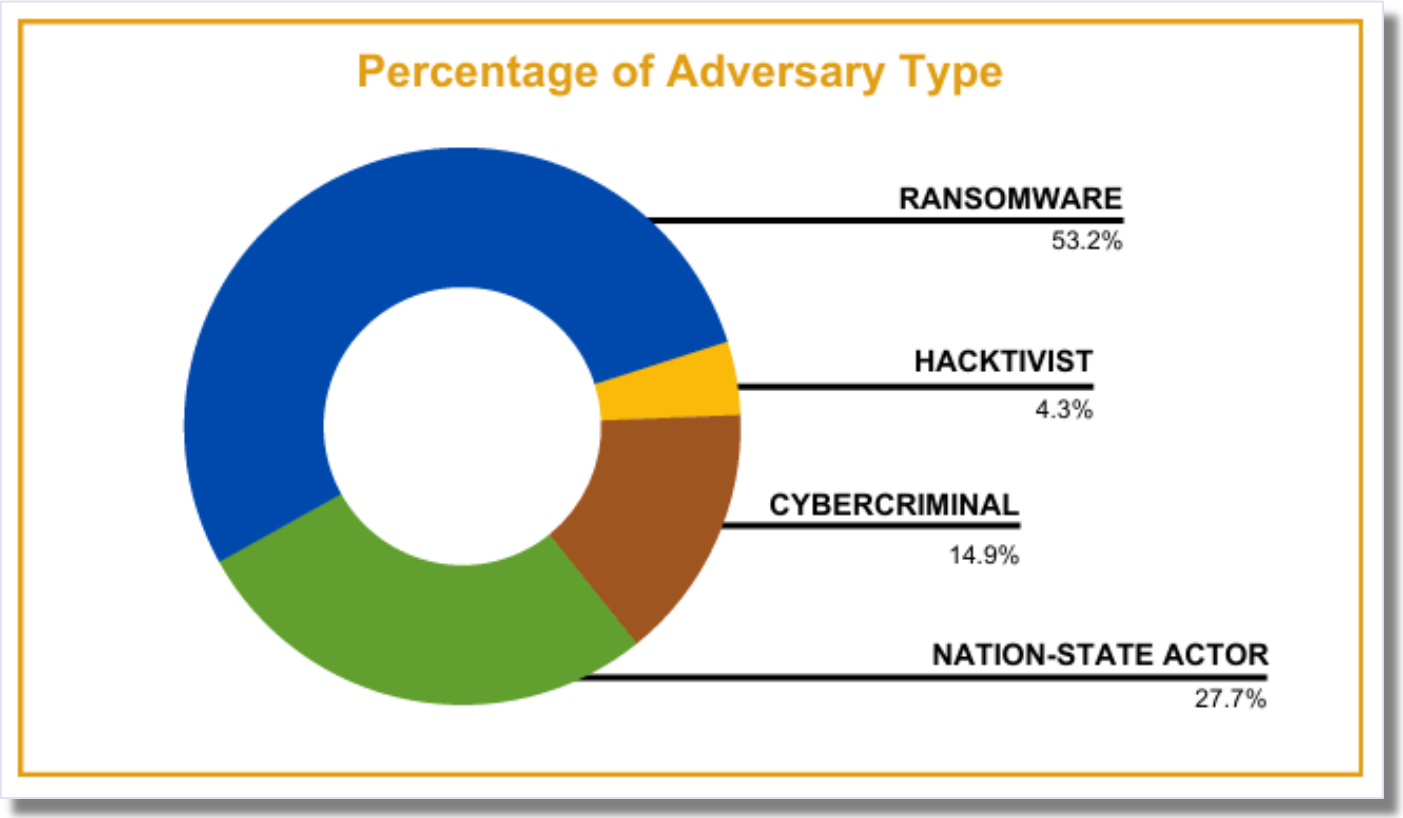
- Artificial Intelligence (AI) and Large Language Models (LLMs) have improved phishing and business email compromise.
- AI powered voicemail phishing has been reported.
- Barrier to entry for would be cybercriminals has been lowered.
  - Automated reconnaissance
  - Malware development
  - Exploitation suggestions

RSAC 2025 Conference

Hacktivists

Hacktivists

- Hacktivists groups may target food and ag sector organizations due to ideological or geopolitical differences.

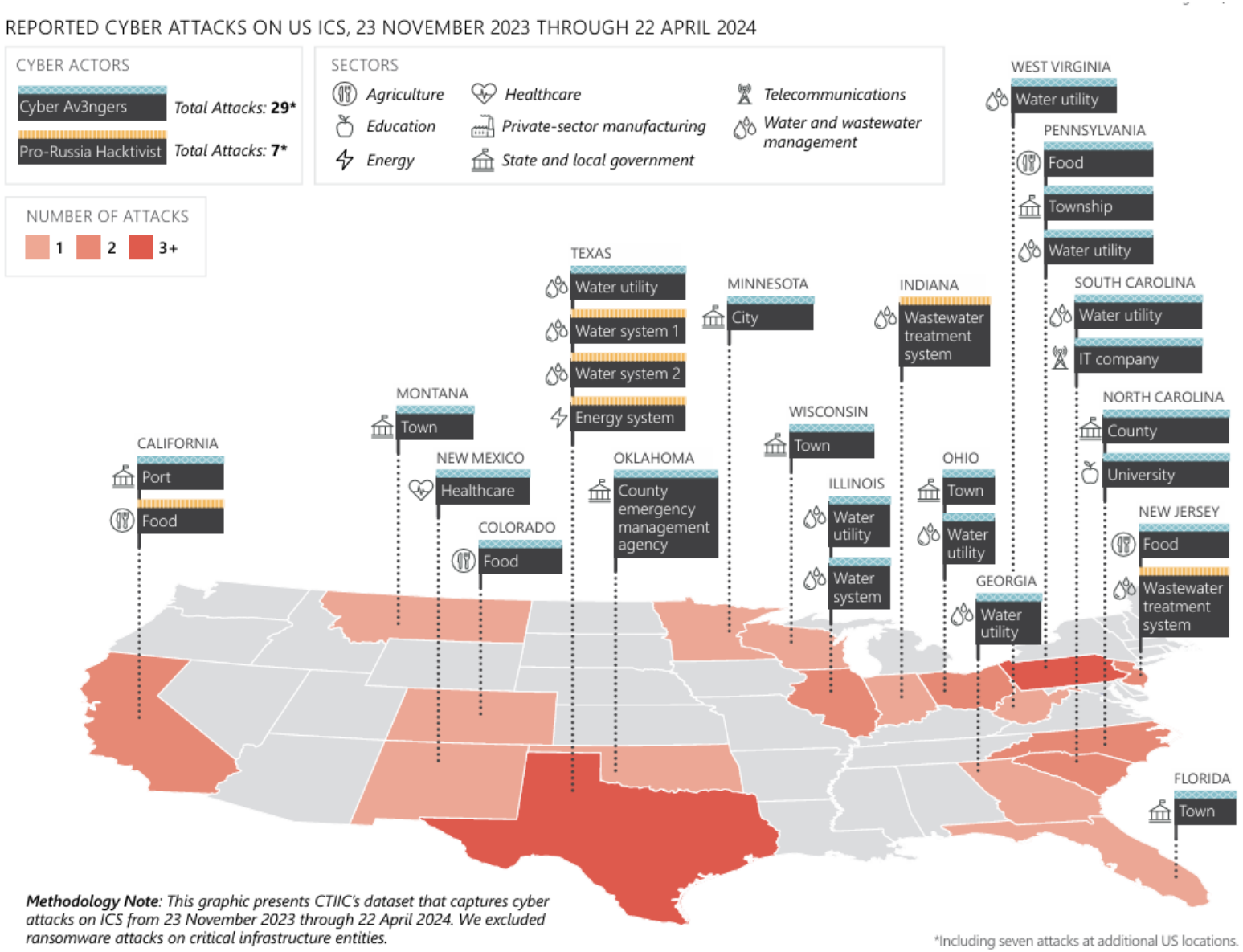


Hacktivists Motivations

- Disrupt critical networks as a means to support their parent countries geopolitically or support ideological allies.
- Attacks can range in severity and sophistication.
- Nuisance attacks
  - Web defacement
  - Distributed denial of service (DDoS)
- Destructive Attacks
  - Wiper Malware
  - Attacks on ICS in critical infrastructure

Hacktivists Motivations

- Current global conflicts have led to the targeting of US critical infrastructure by several hacktivists groups.
  - Notable blurry line between hacktivist and nation-state group who may be leveraging/supporting hacktivists for deniability.
    - Hacktivists potentially receiving support from parent nations
    - State actors masquerading as hacktivist groups
    - Leveraging hacktivism for plausible deniability

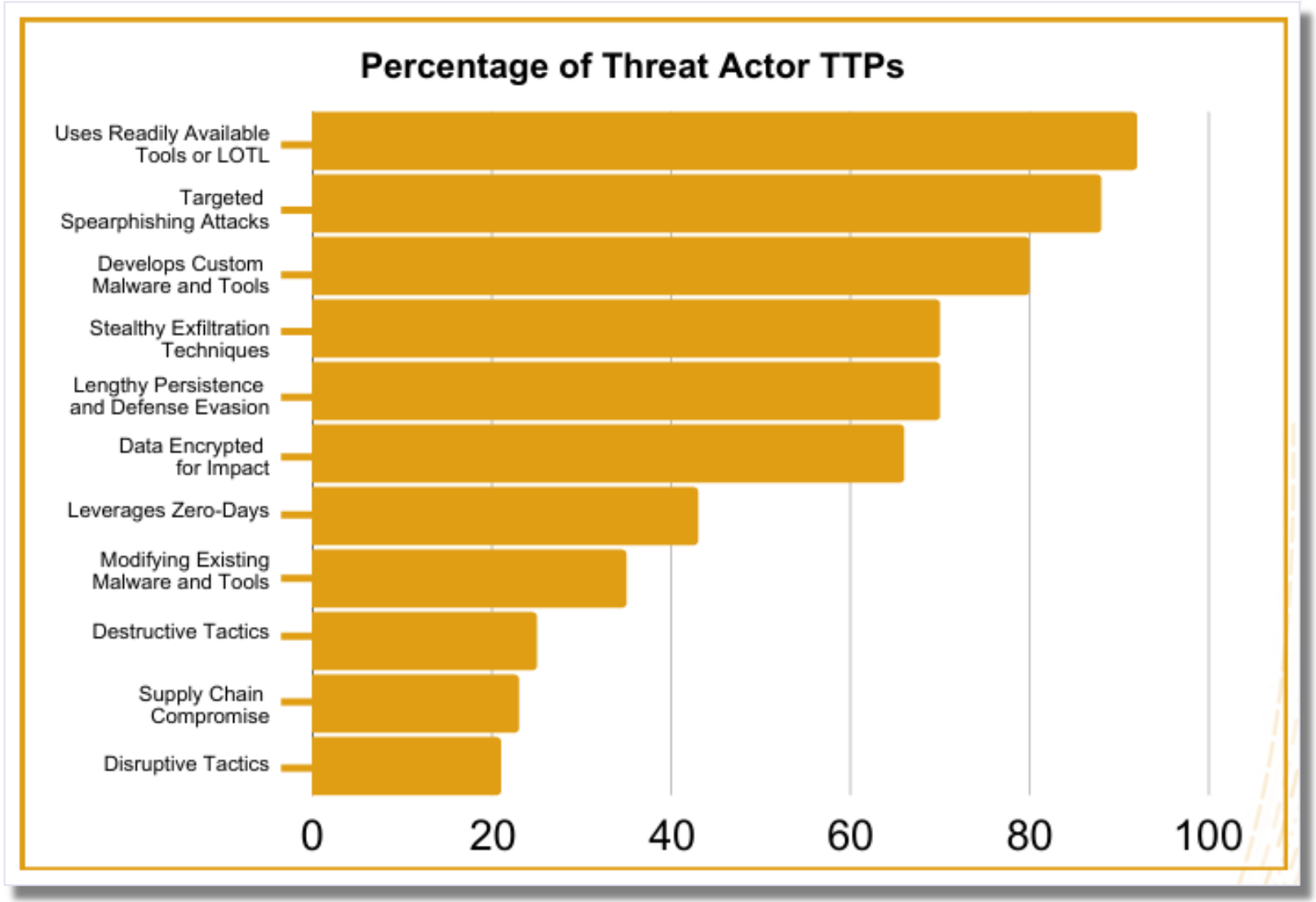


Office of the Director of National Intelligence, 2024

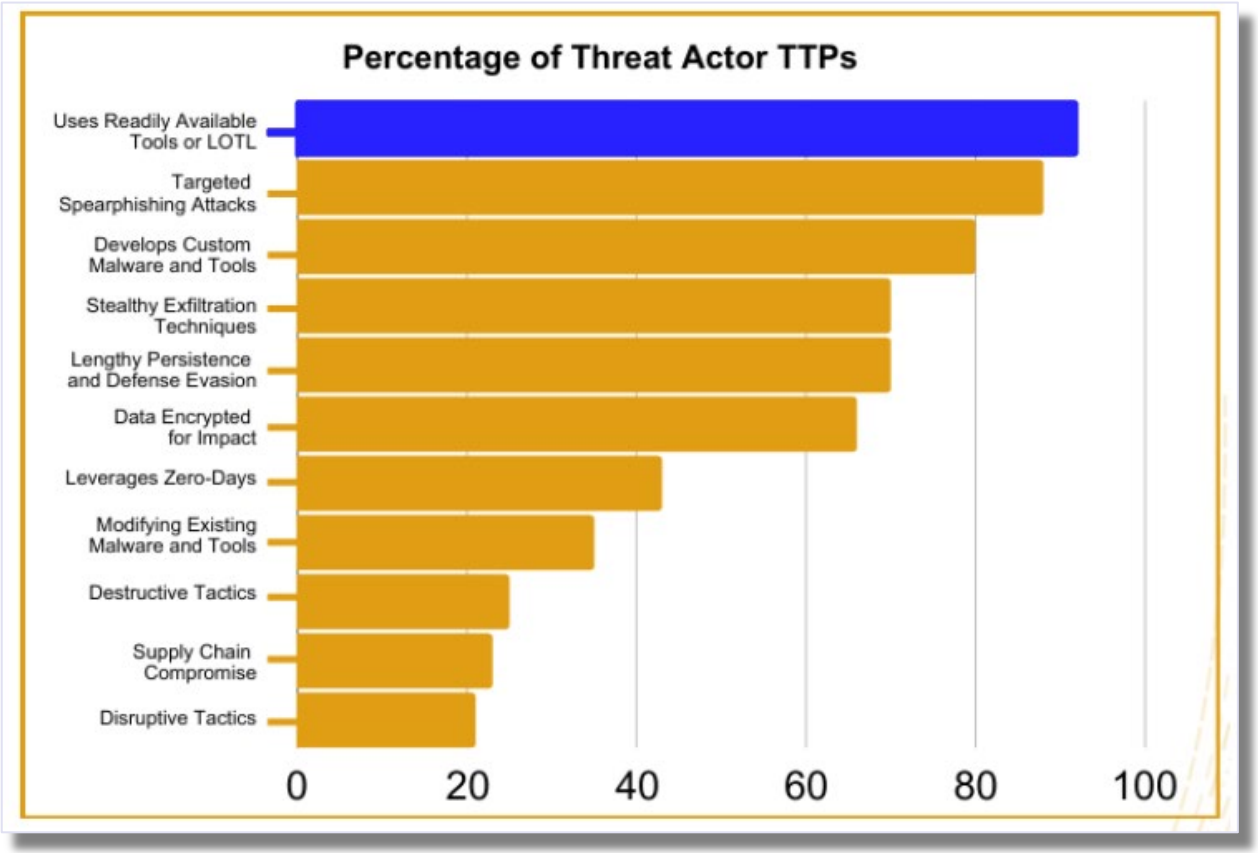
RSAC 2025 Conference

How Are Adversaries Attacking the Food and Ag Sector?

Tactics, Techniques, and Procedures (TTPs)

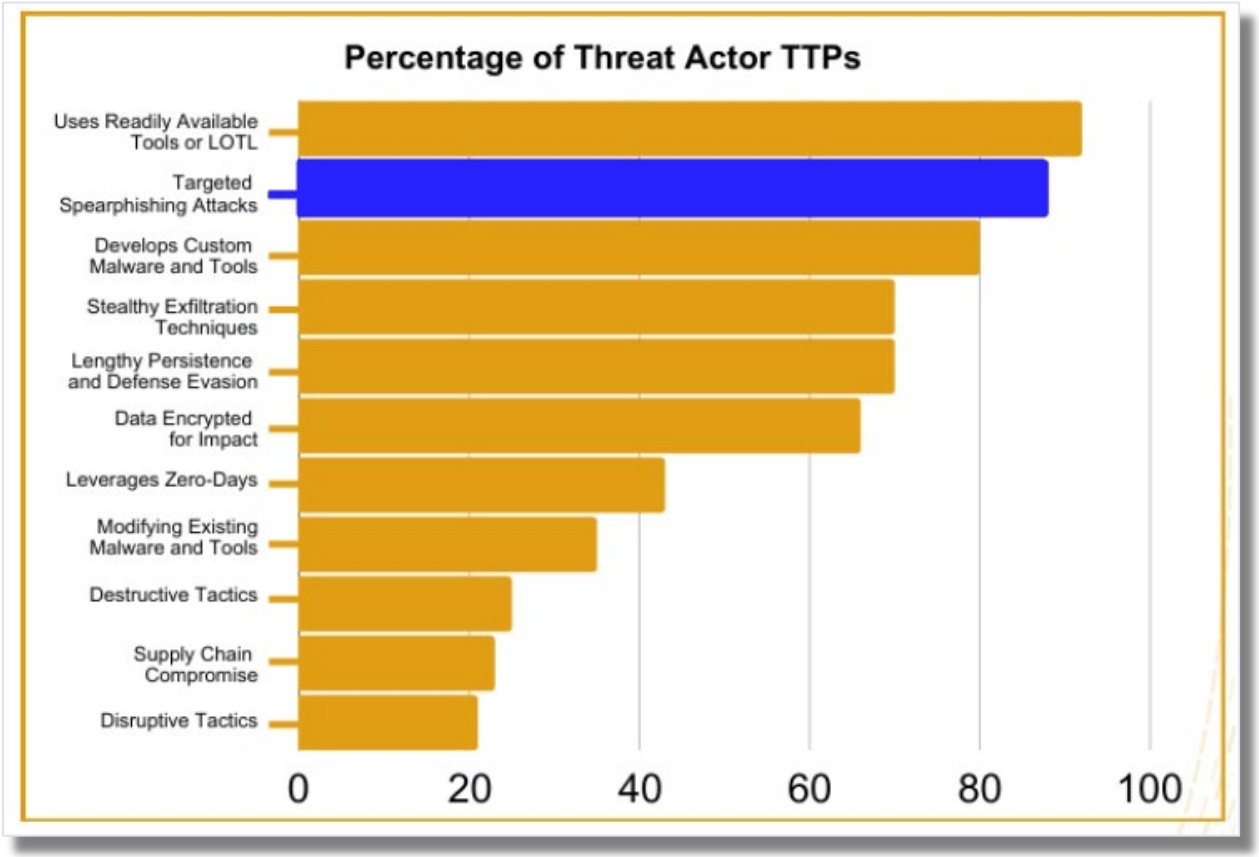


Tactics, Techniques, and Procedures (TTPs)



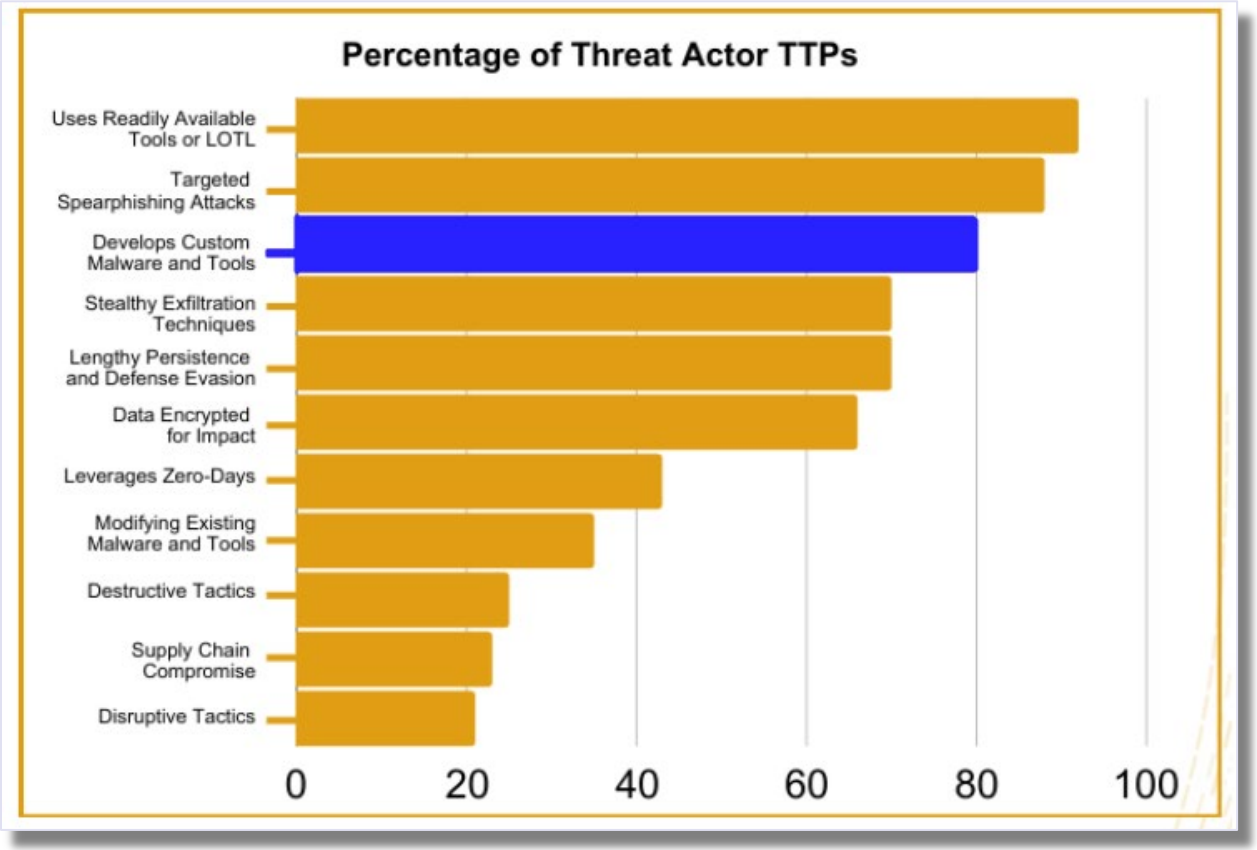
- 92% of the scored adversaries used readily available tools and living-off-the-land (LOTL) techniques.

Tactics, Techniques, and Procedures (TTPs)



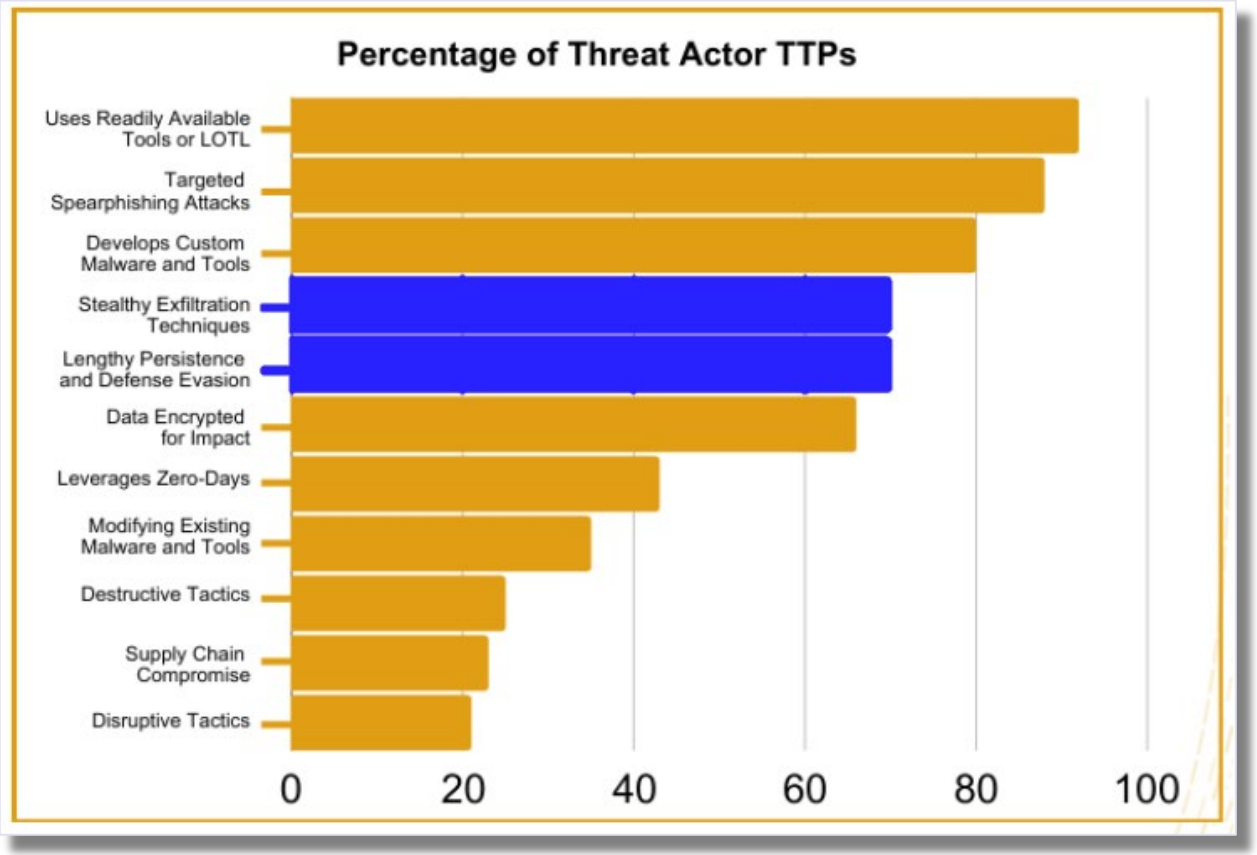
- 88% of the scored adversaries used phishing and spear phishing as a means of initial entry.

Tactics, Techniques, and Procedures (TTPs)



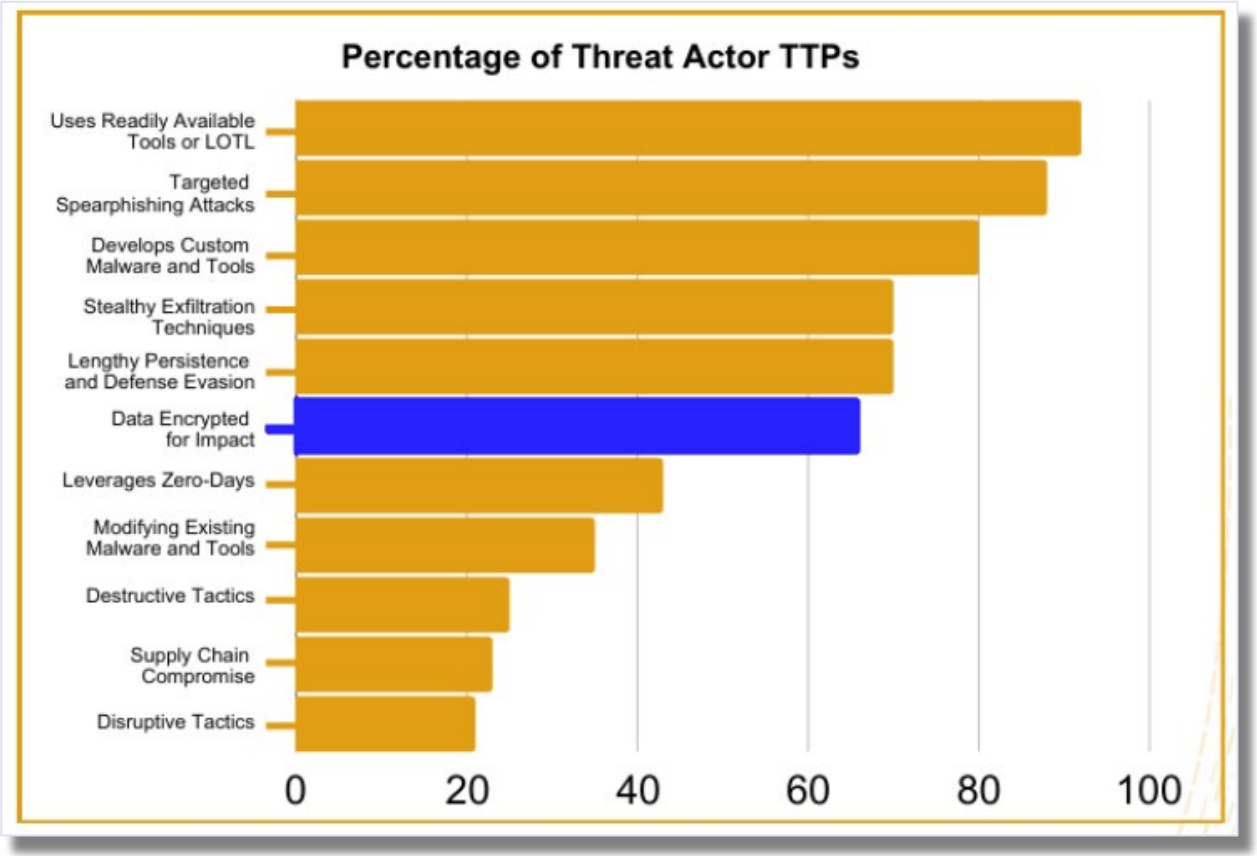
- 80% of the scored groups leveraged custom malware and tools.

Tactics, Techniques, and Procedures (TTPs)



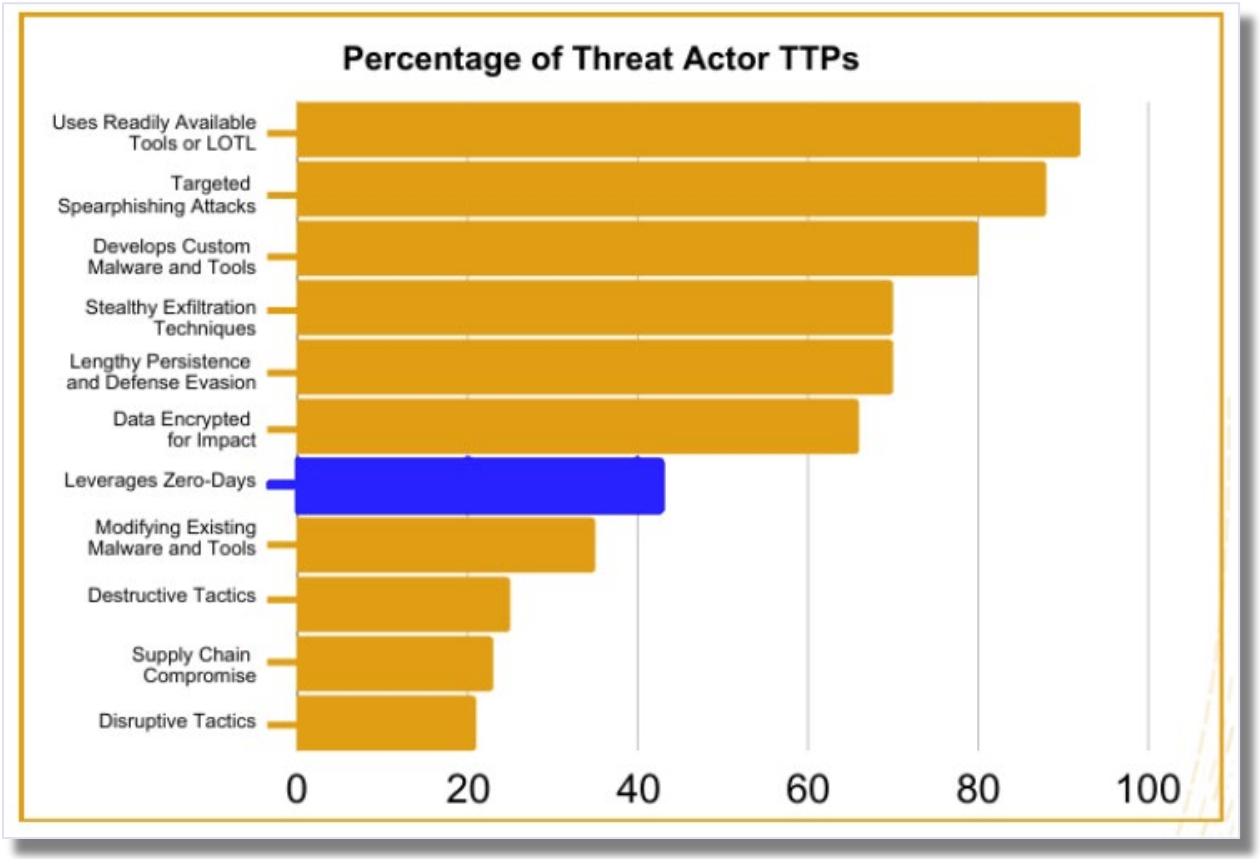
- Lengthy persistence and stealthy exfiltration techniques were used by 70% of the groups we scored.

Tactics, Techniques, and Procedures (TTPs)



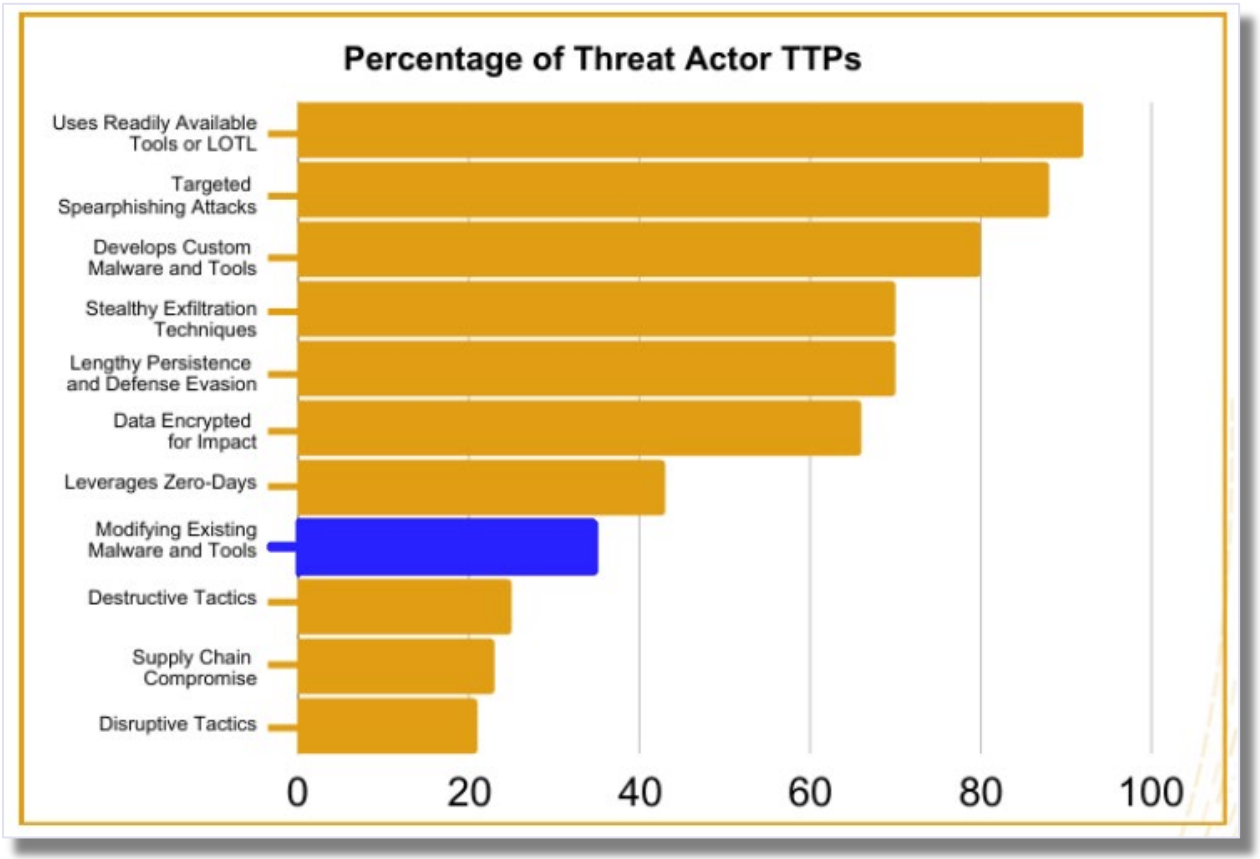
- Data encryption for impact was seen fairly regularly in 66% of scored groups.

Tactics, Techniques, and Procedures (TTPs)



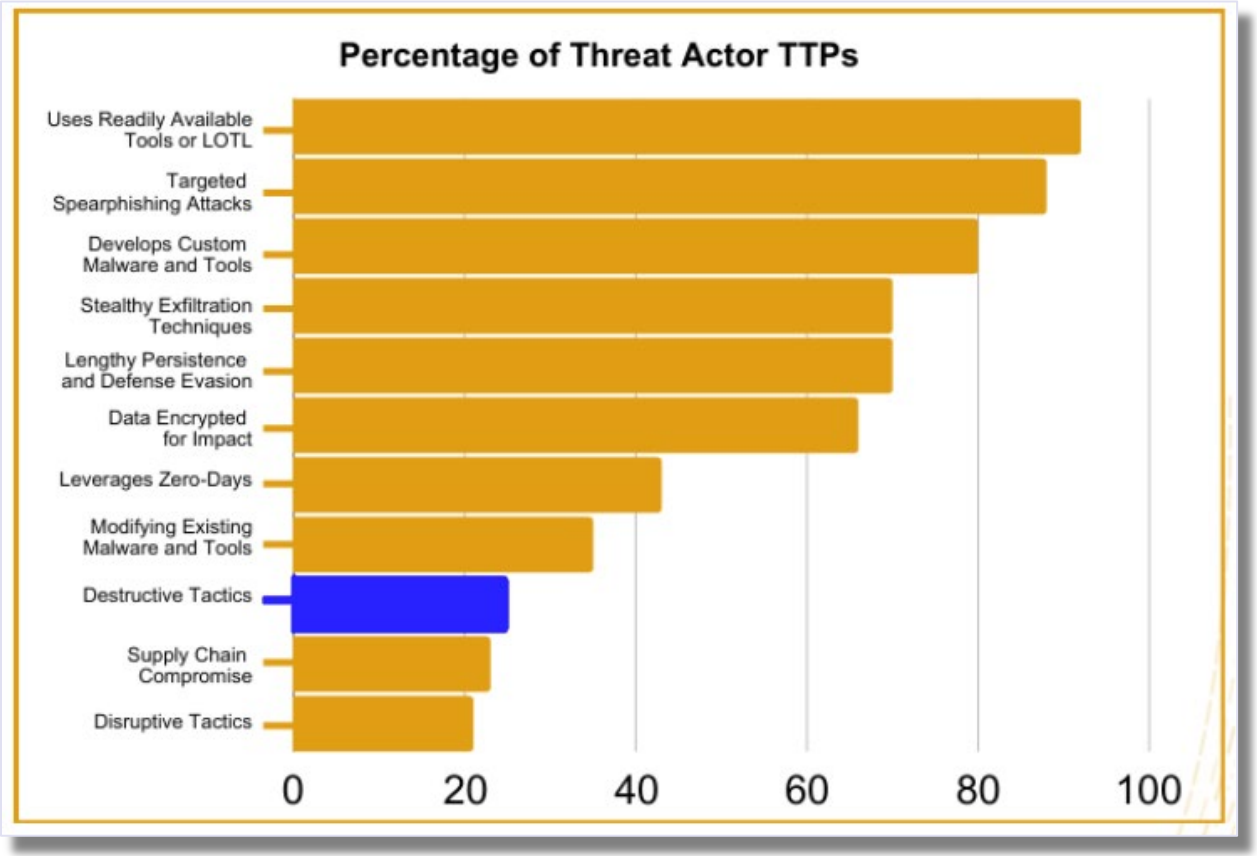
- Only 43% of the groups we scored leverage zero-day vulnerabilities.

Tactics, Techniques, and Procedures (TTPs)



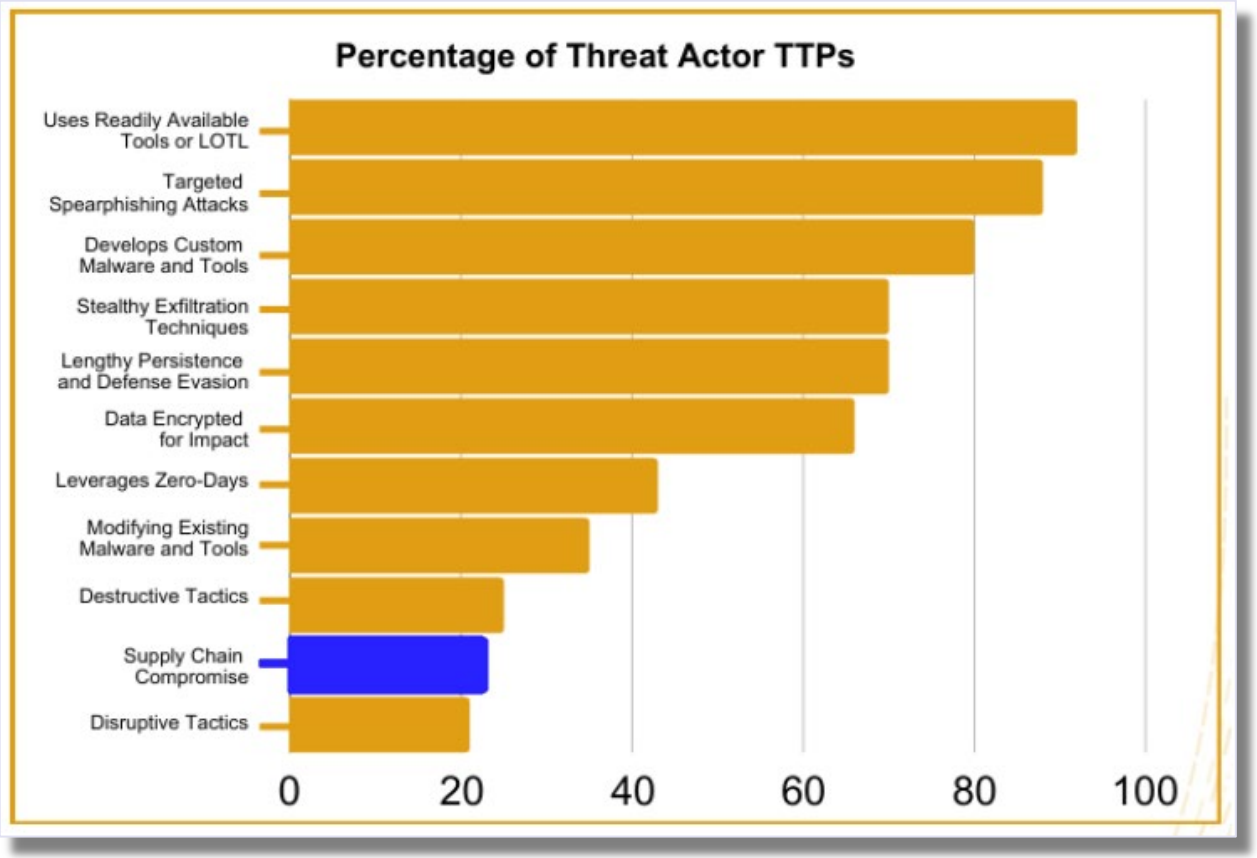
- 35% of adversaries developed their own malware and tools.

Tactics, Techniques, and Procedures (TTPs)



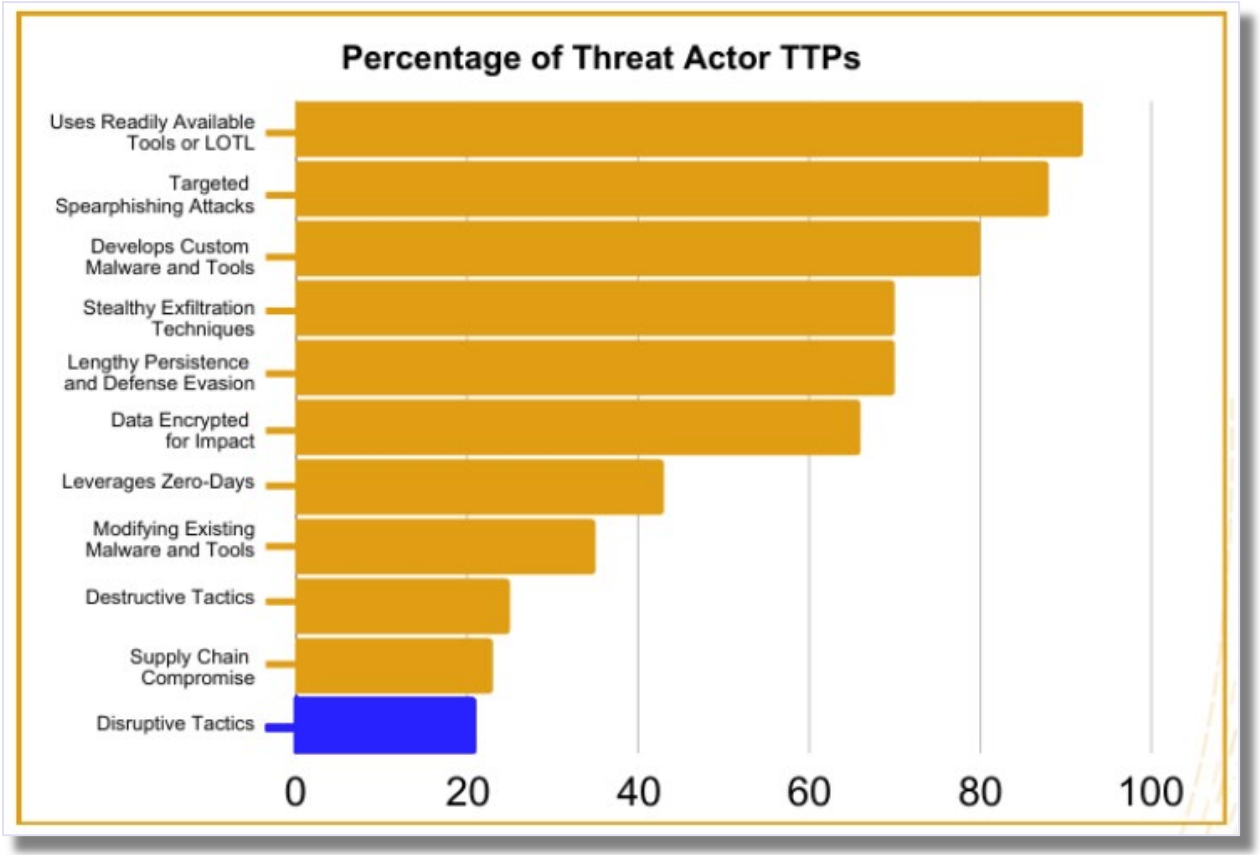
- 25% of adversaries used destruction tactics

Tactics, Techniques, and Procedures (TTPs)



- 23% of the adversaries scored carried out Supply chain compromise.

Tactics, Techniques, and Procedures (TTPs)



- The lowest used tactic on our list was disruptive attacks.

RSAC 2025 Conference

Conclusion

What Did We Learn?

- The Food and Ag sector is no stranger to cyber attacks.
  - Varying adversary motivations dependent on the victim, their size, and their critical infrastructure impact.
  - Ransomware is and will continue to be a problem for all critical sectors.
  - Opportunistic targeting of the sector.
  - Global conflicts could lead to further attacks against critical infrastructure, including the Food and Ag sector.

Apply and Prepare!

- Prepare for “When” not “If” a cyber attack will happen to you.
  - Organizations should continue to educate themselves on specific actors targeting the sector and apply appropriate mitigations based on their common tactics, techniques, and procedures.
- The Food and Agriculture-ISAC will continue to release sector specific intelligence.
  - Quarterly and Yearly Ransomware Reports
  - Sector Specific Threat Reports
  - Cybersecurity Guide for Small and Medium Sized Businesses

General Mitigations

- **Multi-factor Authentication (MFA)**
  - Usernames and passwords are routinely stolen. Add additional factor(s) such as phone with authentication app.
- **Don’t take the Bait!**
  - Defend against phishing and spear phishing.
  - Encourage user awareness and training.
- **Timely Patch Management**
  - Don’t delay patching systems.
  - Threat actors exploit within hours of public disclosure.
- **Network Segmentation**
  - Separate more exposed corporate networks (email) from manufacturing environments.
- **Business Continuity Planning**
  - Prepare and practice, when not if, a cyber event will happen to you.

RSAC 2025 Conference

Many Voices.
One Community.

Thank You

Questions?